Tameside Adult Safeguarding Partnership Board

Managing Allegations against Persons in Position of Trust (PiPoT) Policy

Adapted by Tameside Policy Procedure Subgroup with thanks to Derbyshire and Derby City Safeguarding Adult Boards

Document owner	Tameside Adult Safeguarding Partnership Board Safeguarding Adults Boards
Document author and enquiry point	TASPB Policy and Procedures Group
Document authoriser	Pam Gough
Date of document	2024
Version	1
Document classification	Public
Document retention period	
Next document review date	June 25

Content

Managing Allegations against Persons in Position of Trust (PiPoT)

1.0. Introduction

In response to the Care Act 2014 Care and support statutory guidance - GOV.UK (www.gov.uk), Tameside Adult Safeguarding Partnership Board Safeguarding are required:-

'to establish and agree a framework and process for how allegations against people working with adults with care and support needs (for example, those in positions of trust) should be notified and responded to. Whilst the focus of safeguarding adults work is to safeguard one or more identified adults with care and support needs, there are occasions when incidents are reported that do not involve an adult at risk, but indicate, nevertheless, that a risk may be posed to adults at risk by a person in a position of trust.'

This guidance pertains to situations where an organisation receives information that could impact the suitability of a professional or volunteer to work with adults who require care and support. The information may originate from their activities both within and outside their professional or volunteer roles and workplace. ***Importantly, the alleged victim need not be an adult with care and support needs; it could be a partner or child.*** This guidance addresses scenarios that indirectly involve adults with care and support needs but carry risk implications related to the employment or volunteer work of individuals in positions of trust.

Examples of such concerns could include allegations that relate:

- to a person who works with adults with care and support needs who has:-
    - behaved in a way that has harmed, or may have harmed an adult or child possibly committed a criminal offence against, or related to, an adult or child
    - behaved towards an adult or child in a way that indicates that they may pose a risk of harm to adults with care and support needs.

As with all adult safeguarding work, the Safeguarding Adults Boards (SABs) will work to the following six key safeguarding principles as defined in the Care Act 2014:

- **Empowerment** – Tameside Adult Safeguarding Partnership Board citizens will be supported and encouraged to make their own decisions through informed consent
- **Prevention** – It is better to take action before harm occurs
- **Proportionality** – The least intrusive response appropriate to the risk
- **Protection** – Support and representation for those in greatest need

- **Partnership** – Solutions will come from agencies working together, with all communities in Tameside Adult Safeguarding Partnership Board having a part to play in preventing, detecting and reporting neglect and abuse
- **Accountability** – The work of the Boards will be transparent and accountable

When considering the PIPOT process, it's essential to take into account:

- **Information Sharing**: Ensuring that relevant information is appropriately shared among relevant parties.

- **Employer Responsibilities**: Understanding and fulfilling the obligations and duties of an employer within the context of the process.

- **Risk Assessments:** Evaluating potential risks and implementing measures to mitigate them.

- The Data Protection Act 2018 Complying with the legal requirements outlined in the Data Protection Act 2018.

- General Data Protection Regulation (GDPR)**)**: Adhering to the GDPR guidelines to protect individuals' data rights and privacy.

- Human Rights Act 1998**:** This legislation incorporates the European Convention on Human Rights (ECHR) into UK law. It protects fundamental human rights and freedoms, including the right to privacy, freedom of expression, and the right to a fair trial.

- Crime and Disorder Act 1998**:** This Act addresses various aspects related to crime prevention, youth justice, and anti-social behaviour. It emphasises community safety and aims to reduce crime and disorder.

- Mental Capacity Act 2005 (legislation.gov.uk) The MCA provides a statutory framework to promote the right of individuals to make their own decisions whenever possible. It also protects people who are not able to make their own decisions by defining who can take decisions, in which situations, and how they should go about this. It also enables people to plan ahead for a time when they may lose capacity.

- Care Act 2014 :-This legislation sets out the legal framework for adult social care and support in England.

What is not included:
The following are excluded from this Policy:

- Complaints about a care worker, professional or volunteer where concerns are raised about the quality of practice provided by the person in position of trust, but these do not pose a specific risk to adults or children. Other relevant bodies and their procedures should be used to recognise, respond to and resolve these issues, such as complaints processes or contract management processes. This may also include referral to CQC, NMC, GMC, Social Work England, or similar.

2.0. Assurance to Tameside Adult Safeguarding Partnership Board

Integral to TASPB annual assurance process, each partner agency must provide a statement and evidence that the arrangements for handling allegations against individuals in positions of trust within their organisation are both adequate and functioning effectively.

Cross-organisational challenge will also demonstrate the integrity of the process. In addition, Partner agencies will provide the TASPB Quality Assurance Subgroup with the annual data regarding PIPOT activity in their organisation.

2.1. Safeguarding Adult Board partners

Safeguarding Adult Board Statutory partners for TASPB are defined as:

- Local authority

Tameside MBC

- NHS Greater Manchester

NHS GM | Greater Manchester Integrated Care Partnership (gmintegratedcare.org.uk)

- Greater Manchester Police (Tameside Division)

Tameside | Greater Manchester Police (gmp.police.uk)

These agencies are expected to use this policy within their own organisations, with accountability to TASPB. This means that as well as being responsible for managing risk around any PiPoT concerns about their own staff, where they become aware of potential PiPoT concerns about individuals working for the commissioned agencies, they are responsible for applying this policy and where necessary informing and working with the employer to manage risk.

2.2. Other TASPB partner agencies

Other partner agencies, for example housing providers and voluntary organisations, should ensure their safeguarding leads and managers are aware of this Policy.

2.3. Managing allegations regarding employees

It is expected that every organisation will have appropriate policies and procedures in place to manage allegations against their staff.

- Any allegations should be reported immediately to a senior manager within the organisation.
- Employers should have their own source of advice (including legal advice) in place for dealing with such concerns.
- Where such concerns are raised about someone who works with adults with care and support needs, it will be necessary for:-
    - the employer to assess any potential risk to adults with care and support needs who use their services

    and

    - if necessary, to take action to safeguard those adults.

PIPOT Policies and procedures should be:-

- clear and accessible
- setting out their process for managing risk should they become aware of a PiPoT concern
- determine who should undertake an investigation
- define timescales
- detail how support and advice will be made available to individuals against whom allegations have been made.

2.4. Allegations regarding a potential PiPoT who works outside of Tameside

If the potential PiPoT works outside of the Tameside area, then agencies should familiarise themselves with the relevant Safeguarding Adult Board PiPoT guidance for that area, and make referrals as required.

2.5. Responsibilities when there are potential risks to children

When a person's conduct towards an adult may impact on their suitability to work with, or continue to work with children, this must be referred to the Local Authority Designated Officer (LADO) LADO referral form . Where concerns have been identified about their practice and they are a parent / carer for children, then consideration by the Data Controller should be given to whether a referral to children's services is required.

2.6. Responsibilities of the Data Controller

The receiving organisation becomes the Data Controller as defined by the Data Protection Act 2018 and UK GDPR.

If an organisation is in receipt of information that gives cause for concern about a person in a position of trust, then that organisation should ***give careful consideration as to whether they should share the information with the person's employers to enable them to conduct an effective risk assessment.***

Partner agencies and the service providers they commission, are individually responsible for ensuring that information relating to PiPoT concerns, are shared and escalated outside of their organisation in circumstances where this is required. Such sharing of information must be lawful, proportionate and appropriate. Organisations are responsible for making the judgment that this is the case in every instance when they are the data controller.

If, following an investigation a Person in a Position of Trust is removed, by either dismissal or permanent redeployment, to a non-regulated activity, because they pose a risk of harm to adults with care and support needs, (or would have, had the person not left first), then the employer (or student body or voluntary organisation),

has a legal duty to refer the person to the Disclosure and Barring Service - GOV.UK (www.gov.uk)

It is a criminal offence to fail to make a referral without good reason. This includes situations where if the person in a position of trust resigns, retires or leaves before any investigation is completed. As long as all of the conditions of making a barring referral have been met then this referral should be completed regardless of whether an organisation has accepted or not accepted the person's resignation.

In addition, where appropriate, employers should report workers to the statutory, and other bodies, responsible for professional regulation such as the Health and Care Professions Council, Social Work England, General Medical Council and the Nursing and Midwifery Council where appropriate. Where there is a requirement placed on the professional to self-refer to their regulatory body, this should be reinforced by the employer.

If a person subject to a PiPoT investigation, attempts to leave employment by resigning in an effort to avoid the investigation or disciplinary process, the employer (or student body or voluntary organisation), should conclude whatever process has been utilised with the evidence before them. If the investigation outcome warrants it, the employer can dismiss the employee or volunteer instead and make a referral to the DBS. This would also be the case where the person intends to take up legitimate employment or a course of study.

3.0. Information Sharing

Decisions on sharing information must be justifiable and proportionate, based on the potential or actual harm to adults or children at risk and the rationale for decision-making should always be recorded.

When sharing information about adults, children and young people at risk between agencies it should only be shared:

- where there is a legal justification for doing so (note: this is not the Data Protection Act but comes from underlying legislation**). Where there is a**

suspicion that a crime has occurred, contact should be made with the Police to ensure relevant information is shared.

- where relevant and necessary, not simply all the information held with the relevant people who need all or some of the information
- when there is a specific need for the information to be shared at that time is shared securely

3.1. Timescales

This policy applies whether the allegation or incident is non-recent, or where the information indicates current risk. Whilst there are no specific timescales for managing PIPOT related matters, it is expected that partner agencies respond in a timely manner upon receiving information, depending on the circumstances and risks.

4.0. Legal Framework

Both the Data Protection Act 2018 and the UK GDPR define the following:

Data Subject - an individual who is the subject of personal data.

Personal data is not just about names or addresses, it can be circumstances from which someone can be identified or associated with. The Act does not apply to an individual who has died or who cannot be identified or distinguished from others.

Data Controller - will usually be organisations but can be individuals. In the context of this Policy, the Data Controller is the person/organisation who first becomes aware of the allegation or concern.

The Data Controller is considered to be the owner of the information and has responsibility for taking appropriate action i.e. risk assess and decide whether disclosure to other bodies should be made.

It is the Data Controller that must exercise control over the processing and carry data protection responsibility for it. **The Data Controller must be a "person" recognised in law,** that is to say:

- individuals,

- organisations and
- other corporate and unincorporated bodies of persons

Data Controllers must ensure that any processing of personal data, for which they are responsible complies with Data Protection Act. Failure to do so risks enforcement action, even prosecution and compensation claims from individuals.

Data Processor - In the context of this Policy this is the person who processes the data on behalf of the Data Controller, usually providing a technical service, acting on the instruction of the data controller.

Processing - means use of personal or special category data; everything from the collection of personal data to its eventual disposal.

Data Protection legislation (Appendix 1) requires anyone handling personal information to comply with the principles set out in the Act:

- personal data must be processed fairly, lawfully and in a transparent manner,
- personal data must be processed for specified, explicit and legitimate purposes,
- personal data must only be processed to the extent it is required to do a job; only the minimum must be used,
- personal data must be processed accurately; collected appropriately and kept up-to-date personal data must not be retained for longer than is necessary in an identifiable form and
- personal data must be kept secure

The Information Commissioner's Office (ICO) upholds information rights in the public interest. In addition to complying with the principles, Data Controllers must be accountable for their compliance and be able to support Data Subject Rights. For further information about the law relating to data use/control can be found on their website.

The Crime and Disorder Act 1998 states any person may disclose information to a relevant authority under Section 115 of the Act:

“Where disclosure is necessary or expedient for the purposes of the Act (reduction and prevention of crime and disorder)”

The Human Rights Act 1998

The principles set out in the Human Rights Act must also be considered within this framework in particular the following:

- **Article 6** - The right to a fair trial; this applies to both criminal and civil cases against them …… the person is presumed innocent until proven guilty according to the law and has certain guaranteed rights to defend themselves.
- **Article 7** - A person who claims that a public authority has acted or proposes to act in a way which is unlawful by section 6(1) may a) bring proceedings against public authorities under this act in the appropriate court or tribunal or b) rely on the convention rights or rights concerned in any legal proceedings.
- **Article 8** - The right to respect for private and family life.

Appendix 1: Data Protection Act 2018 and UK GDPR overview

Personal data means data which relate to an identifiable natural person who can be identified from those data, such as name, an identification number, location data, online identifiers or data relating to physical, physiological, genetic, mental, economic, cultural or social identity.

Special category data, in Article 9 of the UK GDPR data means personal data consisting of information as to:

- the racial or ethnic origin of the data subject,
- his / her political opinions,
- his / her religious beliefs or other beliefs of a similar nature,
- whether he / she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
- genetic / biometric data of the purpose of identifying a natural person,
- his / her physical or mental health condition,
- his / her sexual orientation

The Act regulates the “processing” of personal data. Processing in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- organisation, adaptation or alteration of the information or data,
- retrieval, consultation or use of the information or data,
- disclosure of the information or data by transmission, dissemination or otherwise making available,
- alignment, combination, blocking, erasure or destruction of the information or data.

Article 5 of the UK GDPR lists the data protection principles described above.

To determine whether you are a data controller you need to ascertain which organisation decides:

- to collect the personal data in the first place and the legal basis (contained in underlying legislation and other lawful purposes) for doing so,

- which items of personal data to collect, i.e. the content of the data,
- the purpose or purposes the data are to be used for,
- which individuals to collect data about,
- whether to disclose the data, and if so, who to,
- whether subject access and other individuals' rights apply i.e. the application of exemptions and
- how long to retain the data or whether to make non-routine amendments to the data

These are all decisions that can only be taken by the data controller as part of its overall control of the data processing operation.

Appendix 2: Flowchart for Managing Concerns and Allegations against People who Work with Adults with Care and Support Needs